Samlerapport fra Datatilsynets brevkontroll med norske kommuner

Innholdsfortegnelse

Del 1 – Nærmere om brevkontrollene og arbeidsmetodikken til Datatilsynet

Datatilsynet har gjennomført et stort antall tilsyn med norske kommuners etterlevelse av personvernforordningens krav til å ivareta personopplysningssikkerhet. Vi har hatt fokus på å kontrollere kommunenes organisatoriske tiltak som skal virke sammen med tekniske informasjonssikkerhetstiltak.

Datatilsynet sendte den 30. mars 2023 ut likelydende brevkontroller til 93 kommuner og 5 fylkeskommuner, hvor vi ba om redegjørelse om nærmere angitte tema innenfor personvern og personopplysningssikkerhet.

Denne rapporten er en samlet tilsynsrapport for alle de 98 brevkontrollene, og den er basert på de besvarelsene vi har mottatt. Rapporten inneholder beskrivelse av personvernregelverkets krav, oppsummering av besvarelsene vi har mottatt og relevant veiledning om temaene vi har undersøkt.

Datatilsynet gjennomførte i tillegg i oktober 2023 stedlige tilsyn med 10 kommuner, med samme tema som brevkontrollen. Formålet med de stedlige tilsynene var å nærmere kontrollere faktisk etterlevelse på de forskjellige områdene. Det er utarbeidet individuelle tilsynsrapporter for disse tilsynene, og disse er ikke en del av denne fellesrapporten.

1. Bakgrunnen for tilsynene

Norske kommuner og fylkeskommuner er sammensatte og komplekse organisasjoner som behandler store mengder opplysninger om den norske befolkningen i alle livsfaser. Kommunene og fylkeskommunene har et stort ansvar for å ivareta disse opplysningene på en forsvarlig måte.

Alle virksomheter kan utsettes for digitale angrep. Motivasjon og metode bak slike angrep varierer, sammen med alvorlighetsgraden av konsekvenser. Virksomhetens sårbarhet for digitale angrep, og hvor store konsekvensene av et slikt angrep kan være, avhenger også i stor grad av hvor god struktur man har på styring av informasjonssikkerhet og personopplysningssikkerhet. Det nasjonale risikobildet er i kontinuerlig endring, og en god systematikk for ivaretakelse av personopplysningssikkerheten er derfor viktigere enn noensinne.

Datatilsynet har gjennom disse tilsynene gjennomført en større undersøkelse og kartlegging av hvordan norske kommuner ivaretar personvernregelverkets krav til personopplysningssikkerhet.

Formålet med tilsynene er å få kunnskap om modenheten til kommunene og fylkeskommunene knyttet til arbeidet med personvern og personopplysningssikkerhet. Datatilsynet har ønsket å se på generelle tendenser gjennom besvarelsene kommunene har sendt oss.

Datatilsynet ønsker også å bidra til bedre kunnskap om hvordan fylkeskommunene og kommunene i praksis kan oppfylle regelverkets krav og dermed bedre ivareta kravene til personopplysningssikkerhet. En sentral del av denne fellesrapporten inneholder derfor veiledning om de aktuelle temaene.

Målet er at tilsynet og rapporten bidrar til at kommunene blir enda bedre rustet til å håndtere personvernet og sikkerheten rundt personopplysningene til den norske befolkningen.

2. Hjemmel for tilsynene

Tilsynene ble gjennomført med hjemmel i personvernforordningen artikkel 58 nr. 1. Artikkel 58 nr. 1 bokstav a gir Datatilsynet myndighet til å pålegge behandlingsansvarlige å fremlegge all informasjon som er nødvendig for at Datatilsynet skal kunne utføre sine oppgaver.

Datatilsynet kontrollerte fylkeskommunene og kommunenes systematikk for tekniske og organisatoriske tiltak for å ivareta personvern og personopplysningssikkerhet, herunder deres generelle styringssystem og gjeldende retningslinjer, jf. personvernforordningen artikkel 24 nr. 1 og 2, jf. artikkel 32.

3. Gjennomføringen av tilsynene

Datatilsynets undersøkelse av kommunene og fylkeskommunene ble gjennomført som tilsyn i to faser.

Den første fasen er gjennomført som en bred brevkontroll hvor et større antall kommuner har blitt pålagt å besvare spørsmål om etterlevelse av konkrete plikter som følger av personvernregelverket, hovedsakelig i form av dokumenterte rutiner.

I den andre fasen gjennomførte Datatilsynet i løpet av oktober 2023 stedlige kontroller med 10 kommuner. I denne delen av prosjektet fokuserte vi på faktisk etterlevelse i praksis. Kommunene ble valgt ut basert på et representativt utvalg ut fra besvarelsene vi mottok i brevkontrollene, både de som har godt dokumenterte rutiner og de som har etterlatt et inntrykk av at de har mangler eller avvik.

Datatilsynet har utarbeidet individuelle tilsynsrapporter etter de stedlige kontrollene.

4. Datatilsynets krav om redegjørelse

Datatilsynet ba om å få tilsendt følgende:

1. Fylkeskommunen og kommunens behandlingsprotokoll, jf. personvernforordningen artikkel 30.
2. Oversikt over deres organisering av ansvarsforhold knyttet til etterlevelse av personvernregelverket, jf. personvernforordningen artikkel 5 nr. 2.
3. En kort beskrivelse av deres overordnede styringssystem (internkontroll) for etterlevelse av personvernregelverket, herunder hvilke verktøy som eventuelt brukes.
4. Styrende retningslinjer for gjennomføring av risiko- og sårbarhetsanalyser, jf. personvernforordningen artikkel 32.
5. Fylkeskommunen og kommunens eventuelle overordnede sikkerhetsstrategi
6. Oversikt over eventuelle IKT-samarbeid med andre.
7. Styrende retningslinjer for autentiseringsløsninger.
8. Styrende retningslinjer for sikkerhetskopiering og gjenoppretting av systemer, jf. personvernforordningen artikkel 32.1.c).
9. Styrende retningslinjer/prosedyrer for sikkerhetsrevisjoner, jf. personvernforordningen artikkel 32.1.d).
10. Lenke til fylkeskommunen og kommunens personvernerklæring.
11. Informasjon om fylkeskommunen og kommunens personvernombud, herunder:

- navn, telefonnummer og e-postadresse til personvernombudet
- kort beskrivelse av organiseringen av personvernombudsfunksjonen; herunder hvor stor del av full stilling vedkommende skal kunne bruke på utøvelsen av rollen.
- lenke til deres nettside som inneholder informasjon om personvernombudet

5. Om besvarelsene

Fylkeskommunene og kommunene ble gitt en frist på 4 uker til å besvare kravet om redegjørelse fra Datatilsynet. Noen kommuner fikk etter forespørsel innvilget en kort utvidelse på svarfristen.

Det var 5 kommuner som ikke besvarte brevkontrollen.

Datatilsynet har i etterarbeidet sett at våre krav om redegjørelser har vært forstått på forskjellige måter, ettersom besvarelsene varierer i omfang og innhold.

Ettersom besvarelsene gir et noe sprikende datagrunnlag, har kartleggingen vært utfordrende til tross for at vi har vurdert etter oppsatte kriterier. Vi ser likevel noen klare trender/tendenser som vi redegjør for i del to av rapporten. I vår gjennomgang av besvarelsene, har vi overordnet vurdert kommunene etter hvorvidt vi anser besvarelsen som tilstrekkelige, mangelfulle eller manglende.

Vi har i fellesrapporten i all hovedsak vurdert kommunene og fylkeskommunene under ett. Under enkelte punkter omtales fylkeskommunene særskilt, men der dette ikke er gjort er «kommuner» en fellesbetegnelse for både fylkeskommuner og kommuner.

6. Om fellesrapporten

6.1. Presentasjon av de juridiske kravene

Datatilsynet vil i rapporten vise til de relevante rettsreglene som regulerer de konkrete temaene som var gjenstand for tilsynene. Vi gir i tillegg mer utfyllende veiledning om hva de ulike pliktene som følger av regelverket innebærer, og henviser der det er relevant til anerkjent rammeverk.

6.2. Tendenser fra besvarelsene

Datatilsynet har hatt som overordnet mål med tilsynene å vurdere kommunenes og fylkeskommunenes modenhet knyttet til ivaretakelse av personopplysningssikkerhet, og deretter bidra med relevant veiledning på de områdene vi har kontrollert.

I det følgende vil vi presentere hvert enkelt tema vi har vurdert under brevkontrollene, med presentasjon av det juridiske rammeverket, funn fra besvarelsene og med veiledning eller henvisning til nærmere veiledning.

6.3. Veiledningen

Det er utarbeidet omfattende veiledning med god kvalitet av forskjellige aktører på personvernområdet. Datatilsynet har likevel et klart inntrykk av at det er utfordrende for kommuner og fylkeskommuner å navigere i dette landskapet og finne relevant og kvalitetssikret veiledning på de

forskjellige kravene personvernregelverket stiller opp. Datatilsynet har derfor hatt som mål å vise til konkret veiledning innenfor de spesifikke områdene vi har kontrollert.

Vi har også søkt å synliggjøre de konkrete reglene og prinsippene som ligger til grunn for veiledningen. Dette gjør seg særlig gjeldende på delene av kontrollen som retter seg mot konkrete personopplysningssikkerhetstiltak.

I de delene av tilsynene som gjelder organisatoriske og tekniske tiltak som skal baseres på konkrete vurderinger gjort av den enkelte behandlingsansvarlige, har vi vist til veiledning som er knyttet til verktøy som kan brukes av de behandlingsansvarlige ved gjennomføringen av slike vurderinger.

Datatilsynet har hatt som mål å vise til eksisterende veiledning, både på våre egne nettsider og fra andre veiledningsaktører. Vi har valgt å lenke til informasjonen for å sikre at eventuelle oppdateringer blir ivaretatt.

For å begrense omfanget, har vi valgt å vise til konkret veiledning fra anerkjente veiledningsaktører, som har solid kompetanse og erfaring. Aktørene har også etablerte samarbeid med kommunene, og de har kunnskap om kommunene som gjør veiledningen målrettet.

Vi har henvist til veiledning fra følgende aktører:

- Datatilsynet
- Digitaliseringsdirektoratet (Digdir)
- Nasjonal sikkerhetsmyndighet (NSM)
- KS
- Foreningen Kommunal Informasjonssikkerhet (KiNS)
- Norm for informasjonssikkerhet og personvern i helse og omsorgstjenesten (Normen)

Digitaliseringsdirektoratet har tatt initiativ til et arbeid for å utvikle felles sikkerhet i forvaltningen, inkludert en felles referanseramme (eller norm) for arbeidet med informasjonssikkerhet i offentlige virksomheter. Dette er et arbeid Datatilsynet støtter og bidrar inn i, og som vi ønsker å understøtte i denne tilsynsrapporten ved å vise til eksisterende veiledning. Mer om prosjektet «Felles sikkerhet i forvaltningen» kan leses her: https://www.digdir.no/informasjonssikkerhet/felles-sikkerhet-i-forvaltningen/4106

6.4. Eksemplene

Knyttet til de forskjellige temaene i rapporten vil vi vise til konkrete eksempler fra besvarelsene i brevkontrollen. Formålet med å bruke konkrete eksempler, er å vise hva Datatilsynet har vurdert som tilstrekkelig innenfor de forskjellige temaene. Eksemplene er ment som illustrasjon og inspirasjon.

Vi presiserer at disse eksemplene er tilfeldig valgt ut ifra de besvarelsene som ble vurdert som tilstrekkelige innenfor det enkelte temaet. Det er mange som har sendt oss dokumentasjon som kunne ha vært brukt som gode eksempler, men av praktiske årsaker har vi valgt å presentere kun et utvalg av disse. Eksemplene vil legges på https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2023/tilsyn-i-kommuner-og-fylkeskommuner/.

7. Veien videre – hva kan rapporten brukes til?

Datatilsynet har som mål at denne fellesrapporten skal gi en overordnet presentasjon av hvordan norske kommuner og fylkeskommuner ivaretar kravene til personopplysningssikkerhet.

Videre ønsker vi at rapporten skal gi relevant veiledning og dermed et godt grunnlag for de behandlingsansvarliges egen vurdering av om de etterlever personvernregelverket, også for aktører utenfor fylkeskommunal og kommunal sektor.

Vi vil også gi informasjon om erfaringene vi gjør oss under de stedlige kontrollene, og legger til grunn at dette også vil være relevant for alt arbeid med personvern og personopplysningssikkerhet.

Del 2 - Datatilsynets brevkontroll

8. Protokoller over behandlingsaktiviteter

8.1. Datatilsynets krav om redegjørelse

I brevkontrollen ba vi om å få oversendt kommunens behandlingsprotokoll.

Flere kommuner tok kontakt og opplyste om at dette var vanskelig, og at det ville innebære store mengder dokumentasjon. Felles for disse var at de har laget en protokoll pr system som behandler personopplysninger, noe som innebærer at de har mange protokoller.

Det ble avtalt med flere kommuner at de kunne sende en overordnet beskrivelse av hvordan de fører protokoll, sammen med et eksempel.

8.2. Personvernregelverket om behandlingsprotokoll

Plikten til å føre protokoll følger av personvernforordningen artikkel 30. Bestemmelsen angir hvilke aktører som må ha protokoll og hvilke elementer de skal inneholde. Dette omfatter blant annet informasjon om de ansvarlige, formålene, beskrivelse av opplysningene som behandles, eventuelle utleveringer, sletting, sikkerhetstiltak mv.

Artikkel 30 presiserer at protokollene skal være skriftlige, herunder elektroniske. Protokollene skal på anmodning gjøres tilgjengelige for tilsynsmyndigheten.

8.3. Nærmere om kommunenes plikt til å føre protokoll

Kommunen er behandlingsansvarlig for behandling av personopplysninger som skjer i forbindelse med tjenestene de gir til sine innbyggere. De har dermed også plikt til å etablere en behandlingsprotokoll.

En behandlingsprotokoll skal gi kommunen kontroll på alle prosesser som omfatter personopplysninger. Behandlingsprotokollen skal gi en dokumentert fremstilling av hvordan kommunen behandler opplysninger om de registrerte, herunder formålet med behandlingen og behandlingsgrunnlaget.

Kartleggingen at behandlinger av personopplysninger i protokoller er nyttig som del av de ansvarliges internkontrollplikt og dokumentasjon av denne.

Når kommunen for eksempel tilbyr helse- og omsorgstjenester, må det dokumenteres i behandlingsprotokollen hvilke personopplysninger som samles inn om pasienter, brukere, ansatte og pårørende (de registrerte), hvorfor disse personopplysningene må brukes for å tilby tjenesten (formålet), hvorfor kommunen har lov til å behandle personopplysningene (behandlingsgrunnlag) og når opplysningene skal slettes (lagringstid).

Informasjonen i behandlingsprotokollen danner et godt grunnlag for prioritering og systematisering av arbeidet med informasjonssikkerhet i kommunen, både når det gjelder hvilke risiko- og

sårbarhetsanalyser som må utarbeides og hvilke behandlingsaktiviteter som utløser plikt til å gjennomføre en personvernkonsekvensvurdering (DPIA).

8.4. Kommunenes besvarelser

Datatilsynet mottok varierte besvarelser på dette punktet. Enkelte kommuner skrev at oversendelse av protokollene var komplisert. Grunnen til dette var at måten de har bygget protokollene på medførte at dokumentene var veldig omfattende og i et format som det var vanskelig å oversende. Flere sendte etter avtale kun eksempler og beskrivelser av behandlingsprotokollene, mens andre sendte hele protokollen. Enkelte protokoller ble oversendt i et slikt format at de ble uleselige for Datatilsynet.

Mange kommuner benytter verktøy levert av eksterne leverandører til å føre behandlingsprotokoll.

Videre hadde mange kommuner valgt å utarbeide en behandlingsprotokoll for hvert system/løsning de anvender. Dette har medført at noen kommuner har svært mange protokoller.

Flere kommuner har sendt Datatilsynet en rutinebeskrivelse av hvordan protokoller skal opprettes, men ingen eksempler som viser at dette er gjort.

Omtrent 10 % av kommunene informerer om at de ikke har etablert en behandlingsprotokoll. En like stor andel av kommunene opplyser om at deres protokoll(er) har betydelige mangler.

8.5. Datatilsynets vurdering

Personvernregelverket oppstiller ingen formkrav for hvordan en protokoll må se ut eller hvordan den organiseres, utover at det stilles krav til hva den må inneholde. Datatilsynet vurderer derfor at alle de forskjellige måtene og løsningene for behandlingsprotokoll vi har mottatt kan være tilstrekkelige for å etterleve personvernforordningen artikkel 30.

Datatilsynet ønsker imidlertid å påpeke at personvernforordningen artikkel 30 nr. 4 sier at protokollen på forespørsel fra tilsynsmyndigheten skal gjøres tilgjengelig. Kommunene og fylkeskommunene må derfor vurdere om deres løsning for protokoll er egnet for slik tilgjengeliggjøring.

Datatilsynet har ikke etterspurt rutinene for håndteringen av protokollen, og kan derfor ikke vurdere om kommunene og fylkeskommunene har slike ut fra brevkontrollen.

Datatilsynet ser av besvarelsene at kommunene har høy bevissthet om plikten til å føre protokoll. Flere har pågående prosesser med å utbedre eller fullføre utfylling av behandlingsprotkoller som tilfredsstiller personvernforordningens krav.

Det er likevel varierende grad av modenhet, og for Datatilsynet, overraskende stor andel som ikke var der de burde. Vi har anslått at det er omtrent 25-30 % av kommunene som ut fra besvarelsene ikke har tilfredsstillende protokoller.

Datatilsynet anser at personvernforordningen selv gir klare anvisninger om krav til innhold i artikkel 30. Det finnes i tillegg mye tilgjengelig veiledning og støtteverktøy. Vi mener derfor at kravet til å etablere en behandlingsprotkoll er forholdsvis enkelt å etterleve, selv om vi anerkjenner at det innebærer et stort arbeid å gå gjennom alle behandlinger av personopplysninger en kommune gjør.

Vi har også forståelse for at kommunene er komplekse og sammensatte, men dette gjør det desto viktigere å ha dette grunnleggende oversikten på plass.

8.6. Veiledning

Alle virksomheter som behandler personopplysninger, skal føre en protokoll over behandlingsaktivitetene de har ansvar for, ref. plikten nevnt ovenfor.

Det er ikke noen formkrav til hvordan protokollen skal føres, eller hva slags verktøy som skal benyttes. Kommunen kan med andre ord velge om de fører oversikten som et tekstbehandlingsdokument, på regneark, eller ved hjelp av andre verktøy. Kommunene må imidlertid sikre at de svarer ut de obligatoriske kravene til innhold i en samlet skriftlig og elektronisk tilgjengelig oversikt. Protokollen bør være lett tilgjengelig og forståelig, samt at den kan gjøres tilgjengelig for tilsynsmyndighet på anmodning.

Videre skal den behandlingsansvarliges protokoll inneholde følgende informasjon:

1. Navnet på og kontaktopplysningene til den behandlingsansvarlige, og, dersom det er relevant, den felles behandlingsansvarlige, den behandlingsansvarliges representant og personvernombudet.
2. Formålene med behandlingen.
3. En beskrivelse av kategoriene av registrerte og kategoriene av personopplysninger.
4. Kategoriene av mottakere som personopplysningene er blitt eller vil bli utlevert til, herunder mottakere i tredjestater eller internasjonale organisasjoner.
5. Dersom det er relevant, overføringer av personopplysninger til en tredjestat eller en internasjonal organisasjon, herunder identifikasjon av nevnte tredjestat eller internasjonale organisasjon og, ved overføringer nevnt i artikkel 49 nr. 1 annet ledd, dokumentasjon på nødvendige garantier.
6. Dersom det er mulig, de planlagte tidsfristene for sletting av de forskjellige kategoriene av opplysninger.
7. Dersom det er mulig, en generell beskrivelse av de tekniske og organisatoriske sikkerhetstiltakene nevnt i artikkel 32 nr. 1.

En behandlingsprotokoll er et «levende» dokument som til enhver tid skal være oppdatert. Det er viktig å sørge for gode rutiner på gjennomgang og vedlikehold, slik at man sikrer at nye behandlinger av personopplysninger blir oppført. Vurdering av status for behandlingsprotokoll er et naturlig tema i en virksomhets revisjon og rapportering av etterlevelse, som for eksempel i ledelsens gjennomgang.

Datatilsynet har utarbeidet veiledning som blant annet inneholder to enkle maler, for henholdsvis behandlingsansvarlig og databehandler. Se vår veileder for mer informasjon.

Annen relevant veiledning

- Digitaliseringsdirektoratet (Digdir):
  - «Foranalyse».
- KS:
  - «Hva må jeg gjøre før jeg kan ta i bruk ny digital tjeneste?».
  - «Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet».
- Norm for informasjonssikkerhet og personvern i helse og omsorgstjenesten (Normen):
  - «Protokoll over behandlinger av helse- og personopplysninger i virksomheten», faktaark 13.

9. Organisering av ansvarsforhold

9.1. Datatilsynets krav om redegjørelse

Et av formålene med tilsynet var å kontrollere om kommunene og fylkeskommunene ivaretar ansvarlighetsprinsippet, herunder om det er etablert klare rammer for plassering av ansvar og roller. Vi ønsket å undersøke om det er etablert rutiner som gir oversikt og hvordan disse gir den ansvarlige reell styring og kontroll med etterlevelsen av personvernforpliktelsene i hele organisasjonen.

Datatilsynet ønsket under brevkontrollen å undersøke kommunene og fylkeskommunenes bevissthet om kravene til å ha oversikt og styring med det samlede behandlingsansvaret og hvorvidt dette var innarbeidet i styringssystemet deres.

Vi ba derfor kommunene om å sende oss en beskrivelse av kommunens organisering av ansvarsforhold knyttet til etterlevelse av personvernregelverket, jf. personvernforordningen artikkel 5 nr. 2.

9.2. Personvernregelverket om ansvarsforhold

Plikten til å sikre etterlevelse av personvernregelverket retter seg mot den behandlingsansvarlige. Ansvarlighetsprinsippet som er etablert i personvernforordningen artikkel 5 nr. 2 står sterkt, og stiller omfattende krav til blant annet oversiktlige rammer for ansvar og etterlevelse.

Art 24 retter seg mot den ansvarlige, og pålegger at vedkommende skal gjennomføre egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med forordningen.

Kravet om klare ansvarsforhold er også presisert i fortalepunkt 79 som sier at vern av de registrertes rettigheter og behandlingsansvarliges ansvar krever en tydelig fordeling av ansvar.

Forordningens artikkel 32 nr. 4 forplikter videre den behandlingsansvarlige til å treffe tiltak for å sikre at enhver som behandler personopplysninger på deres vegne kun gjør det i tråd med den ansvarliges instruks. Dette gjør det nødvendig å ha oversikt over ansvar og roller.

9.3. Nærmere om ansvarlighetsprinsippet

Den behandlingsansvarlige har stor frihet til å delegere oppgaver og praktisk ansvar for å ivareta kravene etter personvernforordningen. For å ivareta behandlingsansvaret, forutsetter imidlertid slik delegering og fordeling av oppgaver at man etablerer en systematikk som sikrer at man fortsatt har oversikt og kontroll over behandlingene man er ansvarlig for. Slik systematikk gir blant annet den ansvarlige mulighet til å kontrollere etterlevelse. Det er derfor viktig å ha klare beskrivelser av roller, ansvar og oppgaver.

Dette gjelder særlig i en organisasjon med underliggende enheter, hvor det daglige arbeidet med personvern og informasjonssikkerhet ofte er delegert.

Et sentralt tema i styringssystemet til organisasjoner som delegerer ansvar, er systematikken for rapportering tilbake til den behandlingsansvarlige. Slike rutiner er nødvendige for å ha kontroll med at forskjellige tiltak virker etter sin hensikt og er egnede.

Norske kommuner skal ivareta oppgaver på mange samfunnsområder, og er gjerne organisert for best mulig ivaretakelse av disse. Det daglige og praktiske ansvaret for behandling av personopplysninger og informasjonssikkerhet er som regel delegert, både i samsvar med organiseringen til de enkelte fagområdene og til særskilte funksjoner med kompetanse på personvern- og informasjonssikkerhetsområdet.

Oversikt og styring av pliktene som behandlingsansvarlig er derfor en viktig forutsetning for etterlevelse av personvernforordningens krav. I praksis er dette ofte ivaretatt gjennom kommunens styringssystem.

9.4. Kommunenes besvarelse

I Datatilsynets gjennomgang av brevkontrollen har vi undersøkt hvorvidt kommunene har en overordnet oversikt, om de ulike rollene er beskrevet, om de har delegeringsrutiner og om det delegerte ansvaret er tydelig beskrevet. Videre har vi sett på om oppgavene som er delegert har en klar forankring i ledelsen hos den behandlingsansvarlige, blant annet gjennom rapportering, og hvorvidt det delegerte ansvaret er underlagt en god systematikk.

Et flertall av kommunene har sendt oversiktlige beskrivelser av hvordan ansvar og oppgaver for etterlevelse av personvern er ivaretatt, og det er også vedlagt konkrete rutiner for fordeling av ansvar. De fleste som har sendt en oversikt over ansvarsforhold har også besvart tilstrekkelig eller delvis tilstrekkelig på spørsmålet om styringssystem.

16 kommuner har ikke besvart eller sendt utilstrekkelig dokumentasjon på spørsmålet. De fleste av disse har heller ikke et tilfredsstillende styringssystem. Vi ser vi en klar sammenheng med at øvrige områder i kontrollen heller ikke er tilfredsstillende ivaretatt.

Hele 21 kommuner har sendt oss mangelfulle beskrivelser av deres organisering av ansvarsforhold. Manglene vi har merket oss for disse er blant annet at det ikke er vist til konkrete rutiner for organisering og delegering. Enkelte har oversendt korte, overordnede eller overflatiske beskrivelser. Andre har oversendt en beskrivelse av hvordan det *bør* se ut, uten at de har demonstrert at deres kommune har faktiske rutiner for ansvarsplassering. Datatilsynet har også observert mangler ved de besvarelsene hvor ansvarsforholdene er beskrevet fragmentert og hvor det følgelig er lite oversiktlig. Disse har for eksempel beskrevet ansvarsforholdene i dokumenter som sikkerhetsstrategien eller i beredskapsplaner, uten at disse viser ansvarsorganiseringen på en god måte.

Kommuner i samme IKT-samarbeid svarer i mange tilfeller likt på dette spørsmålet. Se nærmere om slike samarbeid i rapportens kapittel 15. Det kan synes som om slike samarbeid øker bevisstheten knyttet til plassering av ansvar. Samtidig ser vi at enkelte samarbeid gjennomgående ikke har redegjort for hvordan de har fordelt ansvar og oppgaver.

9.5. Datatilsynets vurdering

Datatilsynet vurderer at kommunene har høy grad av bevissthet om kravene til oversiktlige og klare ansvarsforhold. Dette kan ha sammenheng med måten kommunen for øvrig har delegert myndighet og oppgaver innenfor sine tjenesteområder.

Det er likevel mange kommuner som bør gjennomgå dokumentasjonen de har og vurdere om de har nødvendig oversikt, beskrivelser og rutiner for å sikre etterlevelse på dette området.

9.6. Veiledning

Norske kommuner skal ivareta oppgaver på mange samfunnsområder, og er gjerne organisert for best mulig ivaretakelse av disse. Gjennom disse oppgavene er kommunen også ansvarlig for behandling av omfattende personopplysninger om sine innbyggere. Dette ansvaret vil i praksis ofte være delegert ut fra en hensiktsmessig organisering av den enkelte kommune. Behandlingsansvaret vil imidlertid fremdeles være plassert hos den øverste ansvarlige i kommunen. For å sikre reell kontroll med at dette ansvaret er ivaretatt, må de forskjellige rollene og ansvaret være tydelig og oversiktlig definert. I tillegg må ansvarslinjene forankres gjennom styringssystemet og i relevante rutiner.

Styringssystemet må sikre at det er sammenhengende ansvarslinjer fra den behandlingsansvarlige og ut til alle som utøver oppgaver innenfor vedkommendes ansvar. I tillegg må kommunen legge til rette for at den ansvarlige kan sikre etterlevelse gjennom systematikk og rutiner for f.eks. rapportering, revisjon og ledelsens gjennomgang.

Datatilsynet har utarbeidet et forslag til innholdet i en ansvarsbeskrivelse.

Annen relevant veiledning

- Digitaliseringsdirektoratet (Digdir):
  - Relevant informasjon om delegasjon og oppfølging gjennom linjen.
- Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen):
  - Omtaler temaet i kapittel 2 i dokument om ledelsens styring og oppfølging.
  - Veileder om internkontroll for informasjonssikkerhet og personvern, særlig kapittel 2.1 omtaler plikten til å ha klare beskrivelser av roller og ansvar, se også kapittel 2.2.2.
- KS:
  - Har omfattende veiledningsmateriell på sine nettsider. I veiledningen «Orden i eget hus» har KS gitt kommunedirektørene en praktisk veileder i internkontrollplikter. Denne veilederens kapittel 2.3 omhandler til en viss grad organisering av ansvar.
  - I tillegg til den generelle veilederen, har KPMG på oppdrag for KS utarbeidet en verktøykasse for informasjonssikkerhet og personvern. Målgruppen er kommunedirektører og fylkeskommunedirektører.

10. Internkontroll / styringssystem

10.1. Datatilsynets krav om redegjørelse

Datatilsynet ba i brevkontrollen kommunene om en kort beskrivelse deres overordnede styringssystem (internkontroll) for etterlevelse av personvernregelverket, herunder hvilke verktøy som eventuelt brukes.

I gjennomgangen av besvarelsene har Datatilsynet tatt høyde for at kommunene kan ha sendt oss et utvalg av informasjon som ikke er representativt for deres faktiske styringssystem. Flere har for eksempel gitt en overordnet beskrivelse uten å vise hvordan de har implementert sitt styringssystem. Andre beskriver hva styringssystemet deres kan eller bør inneholde.

Dette kan ha sammenheng med at vi ba om å få tilsendt en kort beskrivelse, og at dette er tolket på forskjellige måter hos respondentene.

10.2. Personvernregelverket om styringssystem

Den behandlingsansvarlige skal sikre at de grunnleggende prinsippene for behandling av personopplysninger overholdes og skal kunne påvise at dette gjøres, jf. personvernforordningen art. 5 nr. 2.

Ansvaret innebærer en forpliktelse til å gjennomføre egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med forordningen, jf. personvernforordningen art. 24. Det skal i den forbindelse tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter.

Personvernforordningen pålegger den behandlingsansvarlige å iverksette retningslinjer dersom det står i et rimelig forhold til behandlingsaktivitetene, jf. artikkel 24 nr. 2. Bestemmelsen stiller også krav om at tiltakene gjennomgås og oppdateres ved behov, jf. art 24 nr. 1, siste setning og artikkel 32 nr. 1, bokstav d.

10.3. Nærmere om krav til styringssystem

Disse tekniske og organisatoriske tiltakene, omtales ofte som internkontroll, styringssystem eller rammeverk. Rammeverket skal være ledelsens verktøy for å ivareta sitt ansvar og for å kunne demonstrere etterlevelse etter personvernregelverket i sin organisasjon. Tiltakene skal også være de ansattes verktøy for å utføre oppgaver på en forsvarlig og sikker måte.

Regelverket legger opp til en viss skjønnsmargin knyttet til hva som kreves av styringssystemet, ettersom det «skal stå i et rimelig forhold til behandlingsaktivitetene». Det er opp til den behandlingsansvarlige å sikre at systemet er egnet til å oppfylle hensikten med det innenfor den aktuelle virksomheten.

Norske kommuner har en kompleks organisasjonsform med mange underliggende enheter innenfor forskjellige ansvarsområder. Øverste leder er behandlingsansvarlig etter personvernregelverket. En velfungerende og oversiktlig systematikk i organisatoriske og tekniske tiltak er et nødvendig verktøy for den behandlingsansvarlige for å sikre at personvernregelverket er ivaretatt.

En slik systematikk kalles gjerne for styringssystem eller internkontrollsystem. Et velfungerende styringssystem vil gjøre kommunene i stand til å sørge for operasjonell og faktisk etterlevelse, og at de i praksis behandler personopplysninger lovlig, sikkert og forsvarlig.

Det er ikke nødvendig eller hensiktsmessig å etablere en egen internkontroll for personvernregelverket dersom kommunen allerede har en internkontroll for andre regelverk eller for andre formål. Kommunen bør heller sørge for å utvide det eksisterende systemet med elementene som er påkrevd etter personvernregelverket.

10.4. Kommunenes besvarelse

I gjennomgangen av besvarelsene har Datatilsynet vurdert om kommunene har demonstrert at de har et bevisst forhold til sitt styringssystem som verktøy for etterlevelse, og om det fremstår som om slikt system er etablert og i bruk i praksis.

Vi har vurdert hvorvidt kommunene har vist til konkret dokumentasjon, men tatt forbehold om at vårt spørsmål ikke la opp til at dette skulle sendes. Flere kommuner har vist til hva styringssystemet kan inneholde, men ikke hvordan de har fylt systematikken med innhold. Det har ikke vært mulig å gjøre noen kvalitative vurderinger av om systematikken er velegnede.

De aller fleste kommunene har etablerte styringssystemer, av de som har besvart brevkontrollen er det under 10 som kan sies å ikke ha et styringssystem. De aller fleste benytter verktøy for styringssystem som er levert av eksterne leverandører. Flere viser til at de har fulgt veiledningen KS har utarbeidet for internkontroll; *Orden i eget hus.*

Datatilsynet har også observert at det er mange av kommunene som beskriver at de er i pågående prosesser hvor de utbedrer eller endrer sitt styringssystem.

10.5. Datatilsynets vurdering

Tatt i betraktning at Datatilsynet kun har bedt om en overordnet beskrivelse av kommunenes styringssystem, er det vanskelig å gjøre kvalitative vurderinger av besvarelsene. Vi finner det derfor mest hensiktsmessig å fokusere på veiledning knyttet til dette temaet.

10.6. Veiledning

Datatilsynet har en klar forventning om at det er etablert egnede styringssystemer hos alle kommunene. Selv om aktørene varierer i størrelse, er tjenesteområdene tilnærmet like for alle de behandlingsansvarlige. De behandler derfor samme type personopplysninger til samme behandlingsformål, selv om det varierer i omfang.

Det vil imidlertid være forskjeller mellom kommunene som kan påvirke kravene til styringssystemet, for eksempel antall ansatte eller antall innbyggere i en kommune. Dette går frem av ordlyden i forordningen som sier at det skal gjennomføres en helhetlig vurdering før man velger et egnet nivå av tiltak for den enkelte behandlingsansvarlige.

Enkelte elementer vil likevel gjelde for alle kommuner, og vi vil særlig fremheve noen eksempler på forventninger til en kommunes styringssystem. Styringssystemet bør:

- være egnet ut fra definert behov og risiko
- være forankret i ledelse

- ha en klar ansvarsfordeling, delegering og beskrivelse av roller
- være systematisk og oversiktlig
- fremstå praktisk anvendelig og lett tilgjengelig
- ha oppdatert dokumentasjon
- inneholde rutiner for revisjon og gjennomgang

Datatilsynets nettsider inneholder generell veiledning om etablering av internkontroll. Vi har i tillegg konkrete maler og støtteverktøy som kan benyttes i systematikken.

Annen relevant veiledning

- Digitaliseringsdirektoratets (Digdir):
  - Internkontroll i praksis.
- KS:
  - Veilederen «Orden i eget hus».
  - Slik sikrer du oppfølging av personvern og informasjonssikkerhet (utdyper veilederen «Orden i eget hus»).
- KINS Foreningen Kommunal Informasjonssikkerhet (KiNS):
  - Styringssystem.
- Normen for personvern- og informasjonssikkerhet i helse- og omsorgssektoren (Normen):
  - Veileder om internkontroll for informasjonssikkerhet og personvern
  - Normen har også en rekke andre veiledere og faktaark som er relevante i arbeidet med å etablere et egnet styringssystem.

11. Risiko og sårbarhetsanalyser

11.1. Datatilsynets krav om redegjørelse

Vi ba kommunene om å oversende en overordnet/styrende retningslinje for gjennomføring av risiko- og sårbarhetsanalyser. Spørsmålet er relevant da en slik retningslinje vil kunne bidra til at kommunene har en systematisk og konsistent tilnærming til arbeidet med risikovurdering og risikostyring.

11.2. Personvernregelverket om risiko- og sårbarhetsvurderinger

Plikten til å gjennomføre av risiko og sårbarhetsanalyser er forankret i personvernforordningens artikkel 24 og artikkel 32.

11.3. Nærmere om risiko- og sårbarhetsanalyser

Personvernforordningen krever at den behandlingsansvarlige skal beskytte personopplysninger med et egnet sikkerhetsnivå. Dette innebærer at det må gjøres konkrete vurderinger av risiko.

Artikkel 32 omhandler plikten til å ivareta sikkerheten ved behandling av personopplysning, også kalt personopplysningssikkerhet. Kravene innebærer at den behandlingsansvarlige og databehandlere skal gjennomføre tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen. Ved vurderingen av hva som er et egnet sikkerhetsnivå, skal det særlig tas hensyn til risikoene forbundet

med behandlingen, for eksempel som følge av utilsiktet eller ulovlig tilintetgjøring, tap, endring eller ikke-autorisert utlevering av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet.

Krav til gjennomføring av risiko og sårbarhetsanalyser er forankret i personvernforordningens artikkel 24 og artikkel 32, og disse bestemmelsene angir også eksempler på hvilke momenter som må vurderes i slike analyser. Forordningen forutsetter videre at innførte tiltak både skal «sikre og påvise» at regelverket etterleves. Dette forutsetter en systematikk som i praksis etableres gjennom rutiner i et styringssystem. Rutinene må også være egnede for å ivareta kravet, noe som innebærer at de må ha et klart innhold om blant annet ansvar og oppgaver ved gjennomføring av ROS-analyser.

Retningslinjen/rutinen må inneholde overordnet beskrivelse av arbeidet med ROS analyser, f.eks. hvem som har ansvaret, frekvens/hyppighet på revisjon og kontrollaktiviteter (rapportering og oppfølging).

11.4. Kommunenes besvarelse

I gjennomgangen av besvarelsene har vi vurdert om kommunene har sendt oss en overordnet retningslinje for gjennomføring av risiko og sårbarhetsanalyser (ROS). Vi har vurdert om retningslinjen inneholder informasjon om hvem som har ansvaret for risiko og sårbarhetsanalyser, når slike analyser skal gjennomføres, samt hvor ofte disse revideres. Vi har videre undersøkt om retningslinjen inneholdt beskrivelser av kontrollaktiviteter som rapportering og oppfølging.

Fylkeskommunene har utmerket seg med god dokumentasjon og gode beskrivelser av sine retningslinjer. Litt over en tredjedel av kommunene har sendt oss dokumentasjon som viser at de har gode retningslinjer for gjennomføring av risiko- og sårbarhetsanalyser.

I kommunenes besvarelser ser vi likevel at mange av de innsendte retningslinjene er svært fragmentert og beskrevet i ulike dokumenter. Dette gjør at retningslinjene fremstår som lite tilgjengelige, uoversiktlige og vanskelige å navigere i. Dette til tross for at mange kommuner benytter kvalitetssystemer fra levert av eksterne for å holde oversikten over risiko- og sårbarhetsanalyser.

En tredjedel av kommunene har sendt oss mangelfulle retningslinjer (og rutiner) for risiko- og sårbarhetsanalyser. Vi har mottatt mange overordnede beskrivelser av hvordan arbeidet med ROS-analysene er tenkt gjennomført, men uten at de har noen referanser til egen dokumentasjon. Beskrivelsene fremstår som lite forpliktende og er ikke egnet som retningslinjer eller rutiner for å sette organisasjonen i stand til å ivareta sine forpliktelser.

Noen kommuner har sendt oss styrende retningslinjer i tråd med vårt krav i brevkontrollen, andre har sendt gjennomførende rutiner som skjemaer, sjekklister og annet malverk for hvordan risiko- og sårbarhetsanalysene skjematisk skal settes opp.

Den siste tredjedelen av kommunene har helt manglende eller svært utilstrekkelige retningslinjer.

11.5. Datatilsynets vurdering

Vi observerer at majoriteten av kommunene mangler en tilstrekkelig overordnet retningslinje for arbeidet med vurdering av risiko.

Mange kommuner har derimot rutiner og skjemaer for hvordan en risiko- og sårbarhetsanalyse praktisk skal gjennomføres. Vi ser positivt på at kommunene har utarbeidet slike malverk, men

understreker likevel nødvendigheten av en overordnet retningslinje som sikrer en helhetlig systematikk i arbeidet med vurdering av risiko.

11.6. Veiledning

Kommunene har mange behandlingsaktiviteter i mange ulike systemer. I tillegg har de en IKT-portefølje bestående av nye og gamle systemer som er basert på ulik teknologi. Dette gjør kommunens systemlandskap både komplekst og uoversiktlig.

Kommunene skal gjennomføre en risikovurdering før personopplysninger behandles og før man tar i bruk et informasjonssystem. Kommunene skal også gjennomføre risikovurderinger ved endringer i forhold som kan påvirke informasjonssikkerheten, for eksempel i behandlinger, informasjonssystem, eller endringer i trusselbildet.

For å sikre god risikostyring i kommunen anbefaler vi at kommunen utarbeider en overordnet retningslinje for gjennomføring av risikovurderinger. Retningslinjen bør være en del av de styrende dokumentene i internkontrollsystemet og omfattes av ledelsens gjennomgang. Den overordnede retningslinjen bør inneholde informasjon om når og hvordan en risikovurdering skal gjennomføres, hvem som har ansvaret for gjennomføring, oppfølging og rapportering til ledelsen, samt hvilke grenser for risiko som er akseptable (risikoappetitt).

Denne retningslinjen vil kunne bidra til at arbeidet med å avdekke risiko og identifisere risikoreduserende tiltak i kommunen er systematisk og konsistent, og ikke tilfeldig og vilkårlig.

Datatilsynets nettsider inneholder generell veiledning om etablering av internkontroll. Veiledningen inneholder i tillegg konkrete maler og støtteverktøy som kan benyttes.

Hos Datatilsynet kan man også lese mer om hvordan gjennomføre en risikovurdering.

Annen relevant veiledning

- Digitaliseringsdirektoratet (Digdir):
  - Styrende.
  - Gjennomførende.
- Nasjonal sikkerhetsmyndighet (NSM):
  - NSMs grunnprinsipper for IKT-sikkerhet 2.0.
- Foreningen Kommunal Informasjonssikkerhet (KiNS):
  - Prosedyre for risikostyring av informasjonssikkerheten.
- Norm for informasjonssikkerhet i helse og omsorgssektoren (Normen):
  - Veileder om risikostyring i informasjonssikkerhet og personvern.

12. Sikkerhetsstrategi

12.1. Datatilsynets krav om redegjørelse

Vi ba kommunene om å oversende sin eventuelle overordnede sikkerhetsstrategi.

12.2. Personvernregelverket om sikkerhetsstrategi

Personvernforordningen har ingen klare krav til at man må etablere en sikkerhetsstrategi. Det er likevel et organisatorisk tiltak som er å anbefale for å sikre etterlevelse av personvernregelverket.

12.3. Nærmere om sikkerhetsstrategi som tiltak

En sikkerhetsstrategi er en plan for gjennomføring av sikkerhetsarbeidet i en virksomhet. Strategien skal beskrive hvordan de overordnede kravene til sikkerhet (sikkerhetsmålene) skal ivaretas. Sikkerhetsmål og –strategi er virksomhetens overordnede styrende dokument for ivaretakelse av informasjonssikkerhet. En strategi skal bidra til at virksomhetens styringssystem for informasjonssikkerhet er i samsvar med lovkravene i blant annet personvernforordningen.

En velfungerende overordnet strategi bidrar til at kommunenes arbeid med å ivareta informasjonssikkerheten ikke blir tilfeldig og fragmentert, og vil styrke kommunenes evne til å forebygge sikkerhetshendelser.

12.4. Kommunenes besvarelse

I vår gjennomgang av besvarelsene har vi vurdert om kommunene har en overordnet sikkerhetsstrategi, og om denne inneholdt en beskrivelse av roller og ansvar, rutiner for kvalitetssikring og revisjon, samt ledelsens gjennomgang. Vi presiserer at regelverket ikke pålegger konkrete plikter til å ha en slik strategi, noe vi tar høyde for når vi vurderer kommunenes samlede modenhet på dette punktet.

Resultatet av gjennomgangen viser at hele 60 av 94 kommuner har svært mangelfulle eller helt mangler en overordnet sikkerhetsstrategi.

Dokumentasjonen som er sendt oss inneholder i mange tilfeller generelle beskrivelser, uten at de ser ut til å være innarbeidede og spesifikke for kommunen. Beskrivelsene er i mange tilfeller lite forpliktende, korte og overordnede og inneholder lite relevant informasjon om hva som skal gjøres. I mange tilfeller refereres det til dokumenter som ikke er vedlagt eller som i liten grad gir ytterligere detaljer. Disse dokumentene bærer i mange tilfeller preg av å være gamle og utdaterte.

Det er gjennomgående at strategiene mangler beskrivelser av ansvarsfordeling og rutiner for gjennomføring av revisjoner og ledelsens gjennomgang. I de tilfellene denne informasjonen fremgår er det en tendens at beskrivelsene er overfladiske og kortfattede. Vi ser eksempler på at kommunen beskriver behovet for, men ikke de faktiske retningslinjene for revisjon og ledelsens gjennomgang. Slike beskrivelser fremstår som lite håndfaste og konkrete.

12.5. Datatilsynets vurdering

Datatilsynet ser at det er fragmenter av sikkerhetsstrategien i mange ulike dokumenter. Dette gjør arbeidet med å identifisere strategipunktene krevende, og antagelig også vanskelig å jobbe etter i praksis.

Mange besvarelser styrkes av at kommunen har vedlagt eksempler på sikkerhetsinstrukser, sikkerhetstiltak, tiltakskort for å sikre beredskap og annen dokumentasjon som gir inntrykk av at kommunen har et aktivt forhold til arbeidet med å styrke informasjonssikkerheten.

Flere kommuner skriver at de nå har startet arbeidet med å utarbeide en helhetlig sikkerhetsstrategi og har sendt oss sine påbegynte og uferdige utkast. Dette synes vi er veldig positivt.

12.6. Veiledning

Vi anbefaler at kommunene utarbeider en helhetlig og overordnet sikkerhetsstrategi. De strategiske punktene bør samles i et dokument slik at de kan sees i sammenheng. Dette vil lette arbeidet med ledelsens gjennomgang og ved løpende oppdateringer av strategien. Det vil også gjøre det enklere for brukerne å finne frem til, forstå og aktivt benytte strategiens innhold.

En helhetlig sikkerhetsstrategi vil kunne fungere som en veiviser for alle som jobber med å ivareta og styrke informasjonssikkerheten i kommunen. Den vil også kunne bidra til økt forståelse hos brukerne når det kommer til kommunenes satsninger og prioriteringer på informasjonssikkerhetsområdet.

På Datatilsynets nettsider kan du finne informasjon om, samt en konkret mal for, hvordan er slik strategi kan se ut (maler, verktøy, styrende dokumenter).

Annen relevant veiledning

- Digitaliseringsdirektoratet (Digdir)
  - Ledelsens styring og oppfølging.

13. IKT-samarbeid

13.1. Datatilsynets krav om redegjørelse

Vi ba kommunene om å sende oss en oversikt over eventuelle IKT-samarbeid med andre kommuner.

Begrunnelsen for at vi ønsket oversikt over slike samarbeid gjennom brevkontrollen, var at vi ønsket en generell oversikt over utbredelsen. I tillegg ønsket vi å se i hvilken grad (eller om) slike samarbeid har påvirkning på kommunens evne til å etterleve personvernregelverket.

13.2. Personvernregelverket om samarbeid

Dersom kommunenes samarbeid innebærer at de overlater oppgaver knyttet til behandlingsansvaret sitt til andre, må det inngås avtaler om dette. Dette gjelder både for databehandlerrelasjoner og i tilfeller av felles behandlingsansvar.

Bestemmelsene som regulerer dette følger av personvernforordningen artikkel 26-29.

Kommunene har i utgangspunktet stor frihet til å velge hvordan de skal samarbeide, selv om kommuneloven setter noen begrensninger.

Personvernforordningen krever at fordelingen av ansvar og oppgaver er tydelig regulert.

13.3. Kommunenes besvarelse

Et flertall av kommunene skrev at de deltok i et formelt IKT-samarbeid, men har valgt ulike løsninger for dette. Vi kan lese av kommunenes besvarelser at flere samarbeidsformer er representert i denne gruppen:

- Samarbeid som er formalisert gjennom en samarbeidsavtale med en vertskommune etter kommunelovens kapittel 20. Disse formaliserte interkommunale samarbeidene har fokus på å etablere felles IKT strategier og løsninger som ofte omfatter etablering og modernisering av driftsmiljøer, informasjonsforvaltning, infrastruktur og i noen tilfeller driftssentre.
- Samarbeid ved å ha eierinteresser i interkommunale selskap (IKS) eller felleseide aksjeselskaper gjennom en formell skriftlig avtale. Disse selskapene har ofte som oppgave å bidra til å sentralisere, effektivisere og profesjonalisere IKT-driften for kommunene. Omfanget av selskapets oppgaver varierer fra samarbeid til samarbeid. Alle fylkeskommunene som tok del i brevkontrollen svarte at de hadde valgt denne samarbeidsformen.
- Samarbeid ved deltakelse i kommunalt oppgavefellesskap etter kommunelovens kapittel 19. Når slike fellesskap opprettes skal det inngås en skriftlig samarbeidsavtale mellom alle deltakerne i oppgavefellesskapet. Denne samarbeidsformen er tilpasset samarbeid om felles kommunale oppgaver, som for eksempel IKT-tjenester.

Et mindretall av kommunene oppga å ikke delta i et formalisert samarbeid. Ofte har disse allikevel inngått enkelte avtaler direkte med andre nærliggende kommuner i forhold til anskaffelser, felles personvernombud og felles kompetansehevende tiltak. Noen av kommunene i denne gruppen oppgir at fremtidige IKT-samarbeid med andre nærliggende kommuner er under utredning.

Mange kommuner og fylkeskommuner engasjerer seg frivillig i regionale digitaliseringsnettverk. Disse beskrives ofte som et partnerskap mellom kommunene og fylkeskommunen, der målet er gode digitale løsninger for kommunale tjenesteytere og kommunenes innbyggere. Digitaliseringsnettverkene kan bidra til å sette en felles strategisk retning på digitaliseringsarbeidet og tilrettelegge for samarbeid mellom medlemmene.

13.4. Datatilsynets vurdering

Vi ser eksempler på at vertskommuner (jf. kommuneloven kapittel 20) har sendt oss dokumentasjon som i større grad enn andre kommuner blir vurdert til å være tilstrekkelig. Vi kan dog ikke konkludere med at dette er en klar tendens.

Flere kommuner sender likelydende dokumenter som andre kommuner de er i samarbeid med. Enkelte kommuner viser til dokumentasjonen til vertskommunen.

Vi ser en svak tendens til at deltakende kommuner i slike samarbeid i for stor grad hviler seg på vertskommunen, og vi er usikre på graden av etterlevelse i disse kommunene.

Der vertskommunen har levert med høy kvalitet er det heller ikke noen indikasjon på at de deltakende kommunene i samarbeidet leverer samme kvalitet. Kvaliteten er svært varierende og skiller seg ikke fra kommuner som ikke inngår i noe IKT-samarbeid.

13.5. Veiledning

Datatilsynet ser at det å etablere IKT-samarbeid kan ha store fordeler, men det forutsetter at den enkelte kommune er sitt ansvar bevisst, og ikke i for stor grad støtter seg på hva de samarbeidende kommunene gjør. Behandlingsansvaret forblir hos den enkelte kommunen.

Dersom man overlater deler av oppgavene man har behandlingsansvar for til et slikt samarbeid, må kommunene og fylkeskommunene vurdere om det er nødvendig å inngå avtaler i tråd med personvernforordningen artikkel 26-29.

Datatilsynet har utarbeidet veiledning om databehandlerrelasjoner og databehandleravtaler.

Annen relevant veiledning

- Digitaliseringsdirektoratet (Digdir):
  - Vurdere tilgang til data.
- KS:
  - Databehandleravtale til tjenesteavtale.
- Norm for informasjonssikkerhet og personvern i helse og omsorgstjenesten (Normen):
  - Mal for databehandleravtale.
  - Bruk av databehandler (faktaark 10).

14. Autentiseringsløsninger

14.1. Datatilsynets krav om redegjørelse

Vi ba kommunene om å sende oss styrende retningslinjer for autentiseringsløsninger i kommunen. Autentiseringsløsninger har som sin primære oppgave å bekrefte brukerens identitet, og er et subsett av det overordnede tiltaket tilgangsstyring.

Grunnen til at vi ønsket en slik oversikt er at utilstrekkelige autentiseringsløsninger, i særdeleshet løsninger som kun benytter brukernavn og passord som eneste mekanisme er en vesentlig årsak til at uønskede aktører lykkes med å skaffe seg tilgang til virksomheter. Det er også en gjennomgående observasjon at kommunene setter krav til enkelte brukergrupper som ansatte, men utelater å sette autentiseringskrav til privilegerte konti, som system- og administrative brukere. Det er også i stor grad manglende kartlegging av hvilke systemer som krever autentisering, vurdering av kritikalitet på disse og hvilket beskyttelsesbehov disse har.

Dette kan også være en årsak til at uønskede inntrengere etter initiell tilgang (med begrensede rettigheter) over tid kan skaffe seg tilganger med forhøyede rettigheter. Dette gir grunnlag for alvorlige og omfattende brudd på personopplysningssikkerheten ved bl.a. uthenting, manipulering og sletting av personopplysninger fra sensitive løsninger, og noen tilfeller også løsningene for sikkerhetskopiering og gjenoppretting.

Vi ønsket å se i hvilken grad kommunene har effektive retningslinjer for autentisering, som dekker alle systemer og alle brukergrupper, inkludert vurderinger eventuell sterk autentisering (et begrep som også omfatter 2-faktor og multifaktor autentisering).

14.2. Personvernregelverket om autentiseringsløsninger

Personvernforordningens artikkel 32.1.b krever at man skal ha "evne til å sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemene og -tjenestene". Kravene til konfidensialitet kan klart kobles til krav om tiltak for å sikkert bekrefte brukerens identitet for tilgang til systemer som inneholder personopplysninger, og setter også krav til tilgjengelighet.

14.3. Nærmere om krav til autentiseringsløsninger

Dette innebærer at løsningen også skal sikre at gyldige brukere alltid har den nødvendige tilgjengelighet til systemene, noe som er ekstra viktige for systemer som berører liv og helse. Autentisering skal være robust nok til å fungere stabilt over tid og under krevende situasjoner, f.eks. når de er under press fra uønskede aktører.

For å sikre forutsigbarhet rundt hva som regnes som «egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen», bør man ta utgangspunkt i anerkjente rammeverk, for eksempel det internasjonale rammeverket ISO 27001 (krav) og ISO27002 (kontroller) som en referanse. «Grunnprinsipper om IKT-sikkerhet 2.0» (Nasjonal Sikkerhetsmyndighet) er en norsk veiledning som blant annet har koblinger til kontrollpunktene fra ISO 27002, i tillegg til referanser mot andre anerkjente rammeverk.

Datatilsynet har spesifikt tatt utgangspunkt i grunnprinsippene "2.6 Ha kontroll på identiteter og tilganger" som veiledning for hva som være et utgangspunkt for egnede tekniske og organisatoriske tiltak knyttet til autentisering i kommunen. Datatilsynet viser også til KiNS (Foreningen Kommunal Informasjonssikkerhet) ISMS, et styringssystem for informasjonssikkerhet som baserer seg på ISO 27001. Dette styringssystemet inneholder et omfattende bibliotek med maler for dokumentasjon, inkludert retningslinjemaler for tilgangsstyring og autentisering.

14.4. Kommunenes besvarelser og Datatilsynets vurdering

I gjennomgangen av besvarelsene vurderte vi om kommunen har sendt oss tilfredsstillende retningslinjer for autentisering, og hvorvidt den var forankret i anerkjente krav og standarder. Videre vurderte vi om retningslinjene var komplette, strukturerte og hadde et innhold som gjør at de kan fungere som et godt underlag for å frembringe egnede og effektive autentiseringsløsninger tilpasset kommunenes behov.

Datatilsynet har valgt å ikke gjengi kommunenes besvarelser eller våre vurderinger knyttet til dette temaet i samlerapporten. Begrunnelsen for dette er at informasjon om sikkerhetstiltak er underlagt taushetsplikt i medhold av personopplysningsloven § 24, første ledd, annet punktum. Vi har derfor i stedet valgt å fokusere på å gi veiledning i det følgende.

14.5. Veiledning

Mangelfulle autentiseringstiltak kan gjøre kommunene sårbare for forsøk på uønsket tilgang og eventuelt digital utpressing mot egne systemer, samtidig som de potensielt er sårbare for de negative konsekvensene av akkurat slike hendelser.

Effektiv autentisering, og spesielt sterk autentisering, er et av de mest virkningsfulle tiltakene for å redusere sannsynligheten at uønskede aktører kommer inn på virksomhetens systemer, med påfølgende brudd på personopplysningssikkerheten som en mulig konsekvens.

Gjennom retningslinjer skal kommunenes ledelse stille krav til nivå av motstandsdyktighet mot tilfeldige og rettede angrep mot kommunens systemer. Slike retningslinjer vil motvirke at effektiviteten i etablerte tiltak er overlatt til og avhengig av utførende ressurser. Uten retningslinjer vil man kunne skape risiko for store og tilfeldige variasjoner avhengig av enkeltpersoners kapasitet, kompetanse og ressurser (tid og økonomi).

Implementerte autentiseringstiltak kan være gode, grundige og effektive og tilfredsstillende i praksis, selv om det ikke er etablert retningslinjer.

Effektiviteten av en autentiseringsløsning avhenger imidlertid av at man har gode, klare og konkrete retningslinjer for autentisering og en effektiv strategi for overordnet tilgangsstyring, integrert i det overordnede styringssystemet. Disse retningslinjene skal også være utgangspunktet for å kunne utarbeide operative prosesser, prosedyrebeskrivelser og driftsrutiner som skal sikre etterlevelse av retningslinjene. Retningslinjene kan også fungere som underlag for krav og forventninger til tjenestekvalitet på avtaler som gjøres med eksterne parter som leverer autentiseringstjenester.

Datatilsynet ser en trend knyttet til meldinger om brudd på personopplysningssikkerheten ved at hendelser oppstår og uønskede aktører skaffer seg tilgang til virksomhetens systemer ved å utnytte svakheter i autentiseringsløsningene. Den mest åpenbart utnyttede sårbarheten knytter seg til bruken av passord som eneste faktor for autentisering. Passord som eneste faktor har i praksis vist seg å være sårbart fordi en for stor del av løsningens effektivitet overlates til den enkelte brukers subjektive anvendelse av tiltaket.

Såkalte credential stuffing-angrep utgjør en betydelig og mye anvendt sikkerhetstrussel. Dette er en angrepsmetode som utnytter svakheten ved systemer som kun benytter passord og tendensen til å gjenbruke samme brukernavn (ofte epostadresse) og samme passord på tvers av flere tjenester. Ved å bruke stjålne påloggingsdetaljer hentet fra andre tjenester, kan trusselaktører få tilgang til kontoer i virksomhetens egne systemer. Disse angrepene er automatiserte og skjer ofte i stor skala. Sterk autentisering er et effektivt tiltak for å redusere sårbarheten for slike typer angrep.

Passord som eneste faktor kan også medføre at en aktør med tilgang til virksomhetens systemer har gode muligheter til å tilegne seg forhøyede rettigheter over tid. Hendelser av typen «digital utpressing» (ransomware) har svært ofte benyttet seg av svakheter knyttet til autentiseringsløsninger. Løsninger som benytter sterk autentisering (inkl. multifaktor / 2-faktor autentisering) har egenskaper som både gjør at det å skaffe seg en initiell tilgang og å kunne bevege seg skjult i systemene over tid er langt mer krevende. Sterk autentisering vil også kunne gjøre det mer krevende for interne utro tjenere å få uønskede tilganger.

Men sterk autentisering, hvis den kun er implementert på deler av virksomhetens løsninger eller kun for enkelte brukergrupper, risikerer å ikke gir den ønskede beskyttelseseffekt og kan til og med bidra til en følelse av falsk trygghet. Det er også viktig at kommunene ikke bare setter krav til enkelte brukergrupper som ansatte, men også autentiseringskrav til privilegerte konti, som system- og administrative brukere, samt eksterne leverandører. Det er også viktig å ha et bevisst forhold til hvilke konkrete systemer som krever autentisering, vurdering av kritikalitet på disse og hvilket beskyttelsesbehov disse har. Alle relevante klientplattformer må inkluderes, også mobiltelefoner og nettbrett. Det kan også være spesielle brukergrupper som krever spesielle vurderinger av hva som er egnede og effektive tiltak, f.eks. unge barn i skole.

Forskjellige løsninger for sterk autentisering kan også ha forskjellig motstandsdyktighet mot angrep. Det er dokumenterte eksempler på at f.eks. SMS-baserte, men også andre typer sterk autentisering

er blitt omgått. De fleste metoder for sterk autentisering er imidlertid i praktisk bruk bedre enn enkeltfaktor passordbasert autentisering.

I situasjoner med alvorlige brudd på personopplysningssikkerheten vil fravær av retningslinjer eller vurdering av at retningslinjer for autentisering være forhold som regnes som skjerpende.

Datatilsynet anbefaler, basert på NSMs grunnprinsipper, at kommunen etablerer strukturerte retningslinjer for:

- krav til overordnet strategi for hvilke autentiseringsnivåer som skal implementeres for hvilke systemer og hvilke brukergrupper (ønsket beskyttelsesnivå for kommunen)
- krav til kartlegging av virksomhetens systemer og tjenester i kontekst behovet for forskjellige typer autentiseringsnivåer; inkludert mobiltelefoner, nettbrett og annet spesialutstyr
- krav identifisering og kategorisering av de forskjellige brukergrupper og disses behov for forskjellige autentiseringsnivåer; sluttbrukere både i virksomhetens nettverk og fra eksterne lokasjoner, administratorer, systembrukere, eksterne leverandører osv.
- krav til oppdatert dokumentasjon av hvilke systemer som har implementert hvilke autentiseringsnivåer for hvilke brukergrupper
- krav til utarbeidelse av driftsrutiner og prosedyrer for operativ drift av autentiseringsløsningene
- krav om risikovurdering og kvalitetsvurdering av selve autentiseringsløsningene (med bevissthet om at forskjellige løsninger også for sterk autentisering kan ha varierende motstandsdyktighet mot angrep)
- krav til løpende overvåking av og regelmessig revisjon/vurdering av løsningenes effektivitet

Annen relevant veiledning

- Datatilsynet:
  - Bruk av sterk autentisering
  - Biometri
  - Veiledning om credential stuffing-angrep
- Nasjonal sikkerhetsmyndighet (NSM):
  - Grunnprinsipper for IKT-sikkerhet
  - Støtteverktøy for NSMs grunnprinsipper for IKT-sikkerhet 2.0
  - Råd og anbefalinger om passord
- KiNS (Foreningen Kommunal Informasjonssikkerhet)
  - KINS STYRINGSSYSTEM
- Norm for informasjonssikkerhet og personvern i helse og omsorgstjenesten (Normen):
  - Autentisering

15. Sikkerhetskopiering og gjenoppretting

15.1. Datatilsynets krav om redegjørelse

Vi ba kommunene om å sende oss deres styrende retningslinjer for sikkerhetskopiering og gjenoppretting. Disse tiltakene har som sin primære oppgave å sikre tilgjengelighet til og integritet i systemer og data ved uforutsette eller uønskede hendelser.

Begrunnelsen for at vi ønsket en slik oversikt er at evnen til å gjenopprette tilgjengeligheten og tilgangen til personopplysninger dersom det oppstår en hendelse, fremstår som svært varierende i avviksmeldinger som sendes til Datatilsynet. Samtidig fremstår effektivitet og robusthet på dette tiltaket som en viktig suksessfaktor for vellykket og effektiv håndtering av konsekvenser av hendelser. Det kan også bidra betydelig til å redusere kostnadene med etterarbeidet ved hendelser.

15.2. Personvernregelverket om sikkerhetskopiering og gjenoppretting

Personvernforordningen artikkel 32.1.b setter som krav at man skal ha "evne til å sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemene og -tjenestene". Personvernforordningen artikkel 32.1.c setter som ytterligere spesifisering at man har "evne til å gjenopprette tilgjengeligheten og tilgangen til personopplysninger i rett tid dersom det oppstår en fysisk eller teknisk hendelse".

15.3. Nærmere om krav til sikkerhetskopiering og gjenoppretting

Kravene i personvernforordningen gir klare forventninger til å ha systemer for sikkerhetskopiering og gjenoppretting, hvor det er lagt vekt på elementet «evne til gjenoppretting». Dette betyr at tiltaket «sikkerhetskopiering» i seg selv har begrenset verdi hvis ikke elementet «gjenoppretting» er effektivt. I tillegg skal løsningen ivareta den nødvendige tilgjengelighet til systemer og persondata, noe som er ekstra viktige for systemer som berører liv og helse. Systemene skal være robuste nok til å fungere over tid og under krevende situasjoner, f.eks. når de er under press fra uønskede aktører.

For å sikre forutsigbarhet rundt hva som regnes som «egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen», er det relevant og nyttig å utgangspunkt i det internasjonale rammeverket ISO 27001 (krav) og ISO27002 (kontroller) som en referanse. «Grunnprinsipper om IKT-sikkerhet 2.0» (Nasjonal Sikkerhetsmyndighet) er en norsk veiledning som blant annet har koblinger til kontrollpunktene fra ISO 27002, og i tillegg til referanser mot andre anerkjente rammeverk (se «Relevant veiledning» under).

Datatilsynet har spesifikt tatt utgangspunkt i NSMs grunnprinsipp nr. "2.9 Etabler evne til gjenoppretting av data" som veiledning for hva som være et utgangspunkt for egnede tekniske og organisatoriske tiltak knyttet til sikkerhetskopiering og gjenoppretting i kommunen.

15.4. Kommunenes besvarelse og Datatilsynets vurdering

Datatilsynet har valgt å ikke gjengi kommunenes besvarelser eller våre vurderinger knyttet til dette temaet i samlerapporten. Begrunnelsen for dette er at informasjon om sikkerhetstiltak er underlagt taushetsplikt i medhold av personopplysningsloven § 24, første ledd, annet punktum. Vi har derfor i stedet valgt å fokusere på å gi veiledning i det følgende.

15.5. Veiledning

Effektive systemer for sikkerhetskopiering og gode prosedyrer for gjenoppretting er kritiske tiltak for å redusere konsekvensene ved hendelser hvor uvedkommende aktører vellykket kommer inn på virksomhetens systemer. Slike innbrudd kan føre til brudd på personopplysningssikkerheten i form av tap, ødeleggelse eller manipulasjon av data.

Erfaringer fra de siste årene viser at bare en enkelt hendelse kan medføre store kostnader og en betydelig del av disse kostnadene er knyttet til prosesser for gjenoppretting av systemer. I tillegg har naturligvis sikkerhetskopiering og gjenoppretting en vesentlig rolle for å håndtere interne «hverdagshendelser» som skyldes interne uhell eller feil på systemer.

Kommunene må gjennom retningslinjer stille krav til funksjonalitet og robusthet for systemer for sikkerhetskopiering og gjenoppretting, inkludert forventninger til gjenopprettingstid og evnen til å beskytte mot rettede forsøk på å slette eller ødelegge selve sikkerhetskopiene. Retningslinjene bør ha forankring i kommunens styringssystemer for informasjonssikkerhet.

Manglende retningslinjer kan ha betydning for om sikkerhetskopiering og gjenoppretting fungerer som et effektivt tiltak og uavhengig av enkeltpersoners kapasitet, kompetanse og ressurser (tid og budsjetter).

Retningslinjer må dekke både sikkerhetskopieringsprosesser og gjenopprettingsprosesser.

Effektiviteten av sikkerhetskopiering og gjenoppretting avhenger av at man har gode, klare og konkrete retningslinjer, og en effektiv strategi for overordnet sikkerhet, og beredskapsplaner, integrert i det overordnede styringssystemet.

Datatilsynet ser klare trender knyttet til meldinger om brudd på personopplysningssikkerheten at vellykkede hendelser av typen «digital utpressing» (ransomware) har som strategi å slette, kryptere eller manipulere data. Det fremstår også som et mål å få tilgang til og slette data som er sikkerhetskopiert. Dette betyr at man gjør seg selv sårbar ved at man er tvunget til å gi etter for digital utpressing, i stedet for å benytte egne tiltak for å gjenopprette systemer.

Manglende retningslinjer kan føre til at kunnskap om hvordan systemer fungerer i krevende situasjoner, som f.eks. vellykkede digitale utpressingsangrep, er ukjent og avhengig av tilfeldigheter. Retningslinjer skal motvirke sårbarhet gjennom avhengigheten til at de «riktige» personene er tilgjengelige. Etablerte retningslinjer reduserer også sårbarheter knyttet til personavhengig kunnskap og kompetanse til å gjenopprette en sammensatt IKT-portefølje. Porteføljen kan bestå av systemer med komplekse sammenhenger som bør kunne settes tilbake til produksjonsstatus med korrekte programvareversjoner, sikkerhetskonfigurasjoner og med siste korrekte versjoner av datasett med integritet i behold.

Datatilsynet har over tid observert at for en del alvorlige hendelser har det vist seg at sikkerhetskopierte data også har vært mangelfulle, utdaterte og i noen sammenhenger vært svært krevende å tilbakeføre til produksjonsstatus. I noen tilfeller har gjenoppretting tatt dager og uker, heller enn minutter og timer som en korrekt konfigurert løsning kan være i stand til å levere. I de mest kritiske tilfellene har tilbakeføring av siste versjon av sikkerhetskopier ikke vært mulig, og man har måttet basert seg på gjenoppbygging fra mer eller mindre tilfeldige og ofte svært utdaterte kilder.

Kommunen må også definere og spesifisere hvilke datasett som er kritiske og hvilke som er mindre kritiske, og de må tilpasse sine strategier ut i fra dette.

Kostnadene ved slike utfordrende gjenopprettingsprosesser kan bli svært høye, både på grunn av driftsstans og fordi arbeidet i seg selv blir svært ressurskrevende og krever spesialkompetanse. For de mest alvorlige situasjonene er data permanent tapt, til tross for at man trodde fungerende sikkerhetskopiering fant sted.

Kommunen må bør derfor utarbeide krav, strategier og prosedyrer for gjenoppretting av systemer og data. Slike retningslinjer bør inneholde konkrete prosedyrer for gjenoppretting, testing og øvelse hvor man som simulerer faktiske hendelser. Retningslinjene bør også omfatte forventninger til gjenopprettingstid.

Gjenopprettingsprosesser bør sees i sammenheng med tilstøtende tiltak som generelle beredskapsplaner for krisesituasjoner. Dette bør for eksempel omfatte beskrivelser av beredskapsteam, samarbeidspartnere, planer for tilgang til nytt/ekstra utstyr hvis behov og eventuelle tilgang til alternative, midlertidige lokasjoner for IT-systemer ved behov.

Datatilsynet anbefaler, basert på NSMs grunnprinsipper, at kommunens retningslinjer inneholder følgende:

- krav til strukturert kartlegging av systemer og data i kontekst sikkerhetskopiering og gjenoppretting
- krav til verdivurdering av systemer og data
- krav og tilpassede strategier (inkl. hyppighet) for sikkerhetskopiering av forskjellige kategorier datasett
- krav og strategier for sikkerhetskopiering av systemer (programvare, konfigurasjoner, maler og «images»)
- krav og strategier for beskyttelse av sikkerhetskopier (kryptering, tilgangsstyring)
- krav og strategi til (eventuell fysisk) separasjon fra produksjonssystemer
- krav og strategi til testing og revisjon av effektivitet av systemer spesielt i kontekst prosedyrer for gjenoppretting (gjerne tilknyttet simulerte, krevende situasjoner, uavhengig av navngitte enkeltpersoner), øving og testing av disse
- krav og prosedyrer for konkrete gjenopprettingsprosesser
- krav til gjenopprettingstid for forskjellige systemer og data

Annen relevant veiledning

- Nasjonal sikkerhetsmyndighet (NSM):
  - Grunnprinsipper for IKT-sikkerhet.
  - Støtteverktøy for grunnprinsipper for IKT-sikkerhet 2.0.
- KiNS (Foreningen Kommunal Informasjonssikkerhet)
  - KINS STYRINGSSYSTEM
- Norm for informasjonssikkerhet og personvern i helse og omsorgstjenesten (Normen):
  - Sikkerhetskopiering.

16. Sikkerhetsrevisjon

16.1. Datatilsynets krav om redegjørelse

I brevkontrollen ba vi om redegjørelse tilknyttet punkt 4.9 «Styrende retningslinjer/prosedyrer for sikkerhetsrevisjoner, jf. personvernforordningen artikkel 32.1.d)». I dette underkapitlet vil vi ta for oss hva både kommunene og fylkeskommunene har respondert tilknyttet dette punktet.

Punktet er tett knyttet opp til punkt 4.2 (organisering av ansvarsforhold) og punkt 4.3 (styringssystem og internkontroll) i samlerapporten.

16.2. Personvernregelverket om sikkerhetsrevisjon

Kravet til å gjennomføre sikkerhetsrevisjoner er spesifikt forankret i personvernforordningens artikkel 32.1.d). Selve artikkel 32 omhandler sikkerheten ved behandling av personopplysninger, også kalt personopplysningssikkerhet. Lovteksten på dette punktet beskriver at behandlingsansvarlig og databehandler skal gjennomføre tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen, herunder «en prosess for regelmessig testing, analysering og vurdering av hvor effektive behandlingens tekniske og organisatoriske sikkerhetstiltak er».

For å kunne etterleve dette kravet, legger Datatilsynet til grunn at den ansvarlige må etablere egnede rutiner/retningslinjer/prosedyrer, jf. også artikkel 32 nr. 4.

16.3. Nærmere om sikkerhetsrevisjon

Virksomhetene må jevnlig teste, vurdere og evaluere hvor effektive sikkerhetstiltakene de har innført er. En sikkerhetsrevisjon skal omfatte vurdering av organisering, sikkerhetstiltak, og bruk av underleverandører og databehandlere.

Sikkerhetsrevisjon består vanligvis av egenkontroller, internrevisjon og revisjon gjennomført av eksterne parter. Dersom sikkerhetsrevisjonen avdekker bruk av informasjonssystemer som ikke er i tråd med intensjonen, bør det vurderes tiltak for å håndtere situasjonen. Resultatet fra sikkerhetsrevisjon bør dokumenteres og være en del av ledelsens gjennomgang.

I tillegg bør daglig oppfølging av sikkerhetslogger inngå i virksomhetens sikkerhetsrevisjoner. Funn fra loggkontroll bør håndteres som øvrige avvik.

Rutinene for revisjon må være av en slik karakter at de bidrar til at det gjennomføres revisjoner i tråd med kravene i forordningen. Dette innebærer at de må inneholde beskrivelser av prosessen, ansvar for å gjennomføre den, konkrete oppgaver og tidsintervaller, samt hvordan rapportering av resultatene skal formidles til den behandlingsansvarlige/ledelsen.

16.4. Kommunenes besvarelse

I Datatilsynets gjennomgang av brevkontrollen har vi undersøkt hvorvidt kommunene har styrende retningslinjer, fast revisjon, jevnlig revisjoner, oppfølging av revisjonsresultater, klart ansvar for gjennomføring, at det er ledelsesforankret, og om det finnes eksempler på om det er gjennomført tidligere.

Det kommer tydelig frem at en større andel av kommunene, så mange som halvparten, har mangelfull eller svært mangelfull dokumentasjon tilknyttet sikkerhetsrevisjon. Det er flere årsaker til dette.

Oppsummert mener vi at det er gjennomgående at de kontrollerte kommunene mangler konkret dokumentasjon, både styrende og gjennomførende. Vi observerer at det i mange tilfeller er manglende tidfesting for revisjon, manglende rutiner, eller at det kun vises til eksterne databehandlere. Flere kommuner har videre nevnt at dokumentasjonen per dags dato er under arbeid.

Det er i underkant av én fjerdedel som har tilstrekkelig dokumentasjon tilknyttet sikkerhetsrevisjon. Det som kjennetegner disse er at de har helhetlig dokumentasjon med tydelige føringer på gjennomføring og revidering. Sikkerhetsrevisjonen i disse kommunene virker å være godt forankret i ledelsen, og det er konkretisert hvordan revisjonen skal gjøres og hvor ofte. Vi kan se eksempler på at flere av disse kommunene er del av kommunale samarbeid innenfor informasjonssikkerhet og personvern, eksempelvis interkommunale selskaper.

Kun 1 av 5 fylkeskommuner har levert dokumentasjon som anses å være tilstrekkelig på dette punktet. Vi observerer at fylkeskommunene jevnt over mangler dokumentasjon for sikkerhetsrevisjoner. Sikkerhetsrevisjons nevnes i overordnede dokumenter, men konkret dokumentasjon og gjennomførende rutiner mangler.

16.5. Datatilsynets vurdering

Datatilsynet vurdere at kommunene samlet sett i liten grad har tilfredsstillende dokumentasjon tilknyttet sikkerhetsrevisjoner. Det er gjentakende at eksisterende dokumentasjon på dette kontrollområdet er fragmentert. Det mangler konkret og helhetlig dokumentasjon, både styrende og gjennomførende. Videre ser vi at det ofte er mangler tidfesting for revisjon, rutiner, og at det kun vises til eksterne databehandlere og/eller leverandører.

Mange besvarelser styrkes likevel av at kommunen har vedlagt eksempler på sikkerhetsinstrukser, sikkerhetstiltak, tiltakskort for å sikre beredskap og annen dokumentasjon som gir inntrykk av at kommunen har et aktivt forhold til arbeidet med å styrke informasjonssikkerheten.

Det som kjennetegner kommunene som har tilstrekkelig dokumentasjon er at de har tydelige styrende dokumentasjon og klare føringer på gjennomføring. Sikkerhetsrevisjonen i disse kommunene virker å være godt forankret i ledelsen, og det er konkretisert hvordan revisjonen skal gjøres og hvor ofte. Videre kan vi se tendenser på at flere av disse kommunene er del av kommunale samarbeid innenfor informasjonssikkerhet og personvern, eksempelvis interkommunale selskaper.

Blant flere av kommunene som har levert tilstrekkelig dokumentasjon, observerer vi at dokumentasjonen har blitt opprettet svært nylig og i forbindelse med denne brevkontrollen. Dette gir positive signaler med tanke på brevkontrollens effekt.

Videre skriver flere kommuner at de nå har startet arbeidet med å utarbeide en helhetlig sikkerhetsstrategi og har sendt oss sine påbegynte og uferdige utkast. Dette synes vi er positivt.

16.6. Veiledning

Virksomheten skal kontrollere at de tekniske og organisatoriske tiltakene for håndtering av personopplysninger brukes og fungerer etter hensikten. Virksomheten må jevnlig teste, vurdere og

evaluere hvor effektive sikkerhetstiltakene er. En sikkerhetsrevisjon skal omfatte vurdering av organisering, sikkerhetstiltak, og bruk av underleverandører og databehandlere.

Sikkerhetsrevisjon består vanligvis av egenkontroller, internrevisjon og revisjon av eksterne parter. Dersom sikkerhetsrevisjonen avdekker bruk av informasjonssystemet som ikke er forutsatt, skal dette behandles som avvik. Resultatet fra sikkerhetsrevisjon skal dokumenteres og være en del av ledelsens gjennomgang.

Ledelsen skal årlig gjennomgå sikkerhetsmål, sikkerhetsstrategi og organisering av informasjonssystemene. Ledelsen skal kontrollere at disse er i samsvar med virksomhetens behov og eventuelt oppdatere mål, strategi og organisering. Gjennomgangen utføres etter rutine beskrevet i ledelsens gjennomgang.

For mer informasjon, se.

Annen relevant veiledning

- Digitaliseringsdirektoratet (Digdir):
  - Veileder på «Måling, evaluering og revisjon».
- Nasjonal sikkerhetsmyndighet (NSM):
  - «Grunnprinsipper for sikkerhetsstyring», spesielt punkt 3.1 og 3.2.
  - «Veileder for tilsyn med forebyggende sikkerhetsarbeid».
  - «Grunnprinsipper for IKT-sikkerhet».
- KS:
  - «Orden i eget hus», spesielt kapittel 10 og punkt 10.1.
  - «Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet», spesielt kapittel 6 og punkt 6.3.
- Foreningen Kommunal Informasjonssikkerhet (KiNS):
  - Verktøykasse for styringssystem.
  - KiNS sin prosedyre for internrevisjon.
- Norm for informasjonssikkerhet og personvern i helse og omsorgstjenesten (Normen):
  - Sikkerhetsrevisjon, faktaark 06.

17. Personvernerklæring

17.1. Datatilsynets krav om redegjørelse

Datatilsynet ba kommunene om å sende lenke til kommunens personvernerklæring.

17.2. Personvernregelverket om personvernerklæringer

Personvernregelverket pålegger de som behandler personopplysninger å gjøre dette på en åpen måte, og det er flere bestemmelser som spesifiserer dette gjennom plikt til å gi konkret informasjon, jf. for eksempel artikkel 13 og 14. Artikkel 12 i personvernforordningen krever at behandlingsansvarlige gir informasjonen på en klar og tydelig måte. Informasjonen skal blant annet legge til rette for at de registrerte kan utøve sine rettigheter.

17.3. Nærmere om personvernerklæringer

Forordningen oppstiller ikke krav til hvordan man gir informasjon, men personvernerklæringer er en effektiv måte å informere alle om hvordan man behandler personopplysninger og om generelle personvernrettigheter. Informasjonen kan også gis på annen måte, så lenge den oppfyller kravene i forordningen.

Det bør samtidig gis informasjon om hvordan rettighetene kan utøves i praksis, for eksempel hvordan man kan be om innsyn.

17.4. Kommunenes besvarelse

De fleste kommunene har utarbeidet og tilgjengeliggjort informasjon til sine innbyggere gjennom personvernerklæringer. Det er kun 1 kommune som opplyser at de mangler en slik erklæring. Enkelte kommuner har generelle personvernerklæringer og i tillegg konkrete tilpasset definerte tjenesteområder som f. eks. skole.

Enkelte personvernerklæringer ligger lett tilgjengelig på forsiden til hjemmesiden til kommunen, mens andre kan finnes ved å gjennomføre søk.

Noen erklæringer er mangelfulle i forhold til forventningene til informasjonen en kommune må gi til sine innbyggere. Disse bærer preg av å være for overordnede og gir lite utfyllende informasjon. I vår gjennomgang opplevde vi også at enkelte lenker til personvernerklæringen ikke fungerte hensiktsmessig.

17.5. Datatilsynets vurdering

Datatilsynets inntrykk er at kommunene generelt har høy grad modenhet når det gjelder informasjon til sine borgere om behandling av personopplysninger.

Vi anbefaler at alle kommunene gjennomgår informasjonen de har gitt til sine innbyggere for å sikre at de etterlever kravene i regelverket.

17.6. Veiledning

Datatilsynet har utarbeidet veiledning om hvordan informasjon skal gis til de registrerte. Her går vi gjennom overordnede krav og gir nærmere veiledning om hvordan informasjonen må uformes og formuleres.

Datatilsynet har også en egen personvernerklæring som kan brukes som eksempel.

Annen relevant veiledning

- Norm for informasjonssikkerhet og personvern i helse og omsorgstjenesten (Normen):
  - Veileder for rettigheter ved behandling av helse og personopplysninger, særlig punkt 3.3 om retten til informasjon etter personvernlovgivningen.

18. Personvernombud

18.1. Datatilsynets krav om redegjørelse

Datatilsynet ba kommunene om å gi informasjon om kommunens personvernombud. Vi ba om kontaktopplysninger og beskrivelse av hvordan funksjonen er organisert i kommunene. Videre ba vi om at kommunen la ved lenke til kommunens nettside med informasjon om ombudet.

18.2. Personvernregelverket om personvernombud

Personvernforordningen artikkel 37, 38 og 39 slår fast plikten til å etablere personvernombud. Offentlige organer som kommuner er pålagt å utpeke personvernombud, jf. artikkel 37 nr. 1 bokstav a).

Personvernforordningen artikkel 38 nr. 4 angir at de registrerte kan kontakte personvernombudet angående alle spørsmål om behandlingen av deres personopplysninger og om utøvelsen av deres personvernrettigheter.

Artikkel 37 nr. 3 åpner for at flere kommuner på konkrete vilkår kan utpeke et felles personvernombud, og etter nr. 6 åpner bestemmelsen også for at man kan anskaffe tjenesten eksternt gjennom en tjenesteavtale.

18.3. Nærmere om personvernombudsordningen

Personvernombudene er sentrale i virksomhetenes etterlevelse av personvernlovgivningen, og skal ha en uavhengig rolle. Ombudets rolle er å gi råd til ledelsen og andre i virksomheten, men også å kontrollere etterlevelsen av regelverket. I tillegg skal de være kontaktpunkt for de registrerte og Datatilsynet. Dette forutsetter at kontaktinformasjonen til ombudet er tilgjengelig for de registrerte, f.eks. på nettsidene til den ansvarlige eller i personvernerklæringen.

Hensikten med å innføre en obligatorisk ombudsordning i forordningen er å styrke kompetansen om personvernregleverket, samt å sørge for en systematisk oppfølgning av de pliktene forordningen pålegger.

Personvernforordningen gir frihet vedrørende organiseringen av ombud, men forutsetter at ombudet er reelt uavhengig og at den ansvarlige legger til rette for at ombudet skal kunne utføre oppgavene i tråd med vilkårene i regelverket.

18.4. Kommunenes besvarelse

Av de som har besvart er det kun 1 kommune som ikke har etablert ordningen personvernombud. 1 kommune opplyser at stillingen som personvernombud for tiden er vakant.

Det er store forskjeller mellom kommunenes organisering av personvernombudsordningen.

Mange kommuner bruker egne ressurser som personvernombud. Stillingsprosenten som ombud varierer for disse fra 100 % til 3 %. Kommunens størrelse ser ut til å ha betydning for hvor stor stillingsprosent ombudene har.

Flere kommuner deler personvernombud med andre kommuner, og besvarelsene gir inntrykk av at dette er ordninger som er regulert gjennom avtale. Hver av kommunene som deler ombud oppgir at ombudets arbeid utgjør mellom 10-20 % stilling.

Det er også en betydelig andel av de mindre kommunene som kjøper denne tjenesten eksternt. Disse oppgir at tjenesten utgjør mellom 10-20 % stilling.

Fylkeskommunene har alle egne personvernombud i 100 % stilling.

De fleste kommunene har informasjon om personvernombudets rolle og oppgaver på sine hjemmesider, både i personvernerklæringen og som konkret informasjon. De fleste oppgir også kontaktinformasjonen til personvernombudet.

18.5. Datatilsynets vurdering

Kommunene har gjennom tilsynene vist at de har implementert personvernombudsordningen, selv om det er forskjellige løsninger for hvordan den er organisert.

Temaet for tilsynene var å få en oversikt over i hvor stor utstrekning ombudsordningen var implementert i kommunene. Vi har ikke gjort en kvalitativ vurdering av innholdet i kommunenes personvernombudsordninger.

Informasjon om ombudet og hvordan man kan komme i kontakt er en sentral forutsetning for at ordningen skal virke etter sin hensikt, og det fremstår som om kommunene i stor grad er bevisste på dette.

18.6. Veiledning

Datatilsynet har utarbeidet forholdsvis omfattende veiledning om personvernombudsordningen.

På disse sidene finnes det blant annet informasjon hvem som plikter å ha personvernombud, hvilke kvalifikasjoner disse må ha og hvordan de ansvarlige skal legge til rette for at ombudene skal kunne utføre oppgavene sine.